

ABSTRACT

A technique based on the use of a quantifier elimination decision procedure for real closed fields and simple theorem proving to construct a series of successively finer qualitative abstractions of hybrid automata is taught. The resulting abstractions are always discrete transition systems which can then be used by any traditional analysis tool. The constructed abstractions are conservative and can be used to establish safety properties of the original system. The technique works on linear and non-linear polynomial hybrid systems: the guards on discrete transitions and the continuous flows in all modes can be specified using arbitrary polynomial expressions over the continuous variables. An exemplar tool in the SAL environment built over the theorem prover PVS is detailed. The technique scales well to large and complex hybrid systems.